IN THE CLAIMS

Please cancel claims 2, 4-6, 13, 16-18, 26, and 33-34 and amend the remaining pending claims to read as follows:

1. (Currently Amended) Á method of selectively making information available to groups of parties amongst a plurality of parties, said method comprising the steps of:

a) generating at least one public key, each having a recognizable name portion;

b) publishing said public key;

c) generating at least one random suffix serving as a secure key;

d) combining said secure key with said public key by concatenating ones of said random suffixes with ones of said public keys; and

e) distributing a key corresponding to said secure key to members of a selected group.

3. (Currently Amended) A method as in claim 1, wherein in step (d) said secure key is combined with each of said plurality of public keys.

7. (Currently Amended) A method as in claim 1, wherein in the distribution step (e), each of said random suffixes is sent as its corresponding key to members of at least one selected group, at least one selected group not receiving at least one distributed key.

8. (Currently Amended) A method as in claim 7, wherein group members use said received random suffixes to access secure information.

9. (Original) A method as in claim 8, wherein the secure information is contained on a web page, each web page containing secure information being identified by one of said random suffixes.

10. (Currently Amended) A method as in claim 1, wherein the random suffixes are encryption keys and the corresponding keys are decryption keys.

11. (Currently Amended) A method as in claim 10, further comprising creating at least one secure web page, each having a secure web page name.

12. (Original) A method as in claim 11, wherein the step (e) of distributing the decryption keys to group members further comprises sending e-mail to members of the selected group, informing said members of said secure web page name.

14. (Currently Amended) A method as in claim 1, wherein the secure keys are encryption keys and the corresponding keys are decryption keys.

15. (Currently Amended) A method as in claim 14, wherein said encryption keys are combined with one or more links, said links combined with encryption keys being published as encrypted links.

19. (Currently Amended) A method as in claim 11, said method further comprising the step of:

f) changing secure page names for a selected group.

20. (Currently Amended) A method as in claim 19, wherein the step (f) of changing secure page names comprises the steps of:

i) removing a secure key from said secure page name;

ii) attaching a new random suffix; and

iii) sending e-mail to members of said selected group, informing said members of said name change.

21. (Currently Amended) A method as in claim 1, wherein the step (c) of generating the random suffix comprises the steps of:

i) generating a plurality of random numbers; and

ii) mapping each of said plurality of random numbers to a corresponding alphanumeric character.

22. (Original) A method as in claim 21, wherein each of said random numbers is a number between 0 and 61.

23. (Original) A method as in claim 22, wherein the mapped plurality of random numbers generated is a decryption key, the method further comprising:

iii) deriving an encryption key from said generated decryption key.

24. (Currently Amended) A computer program product for selectively making information available to selected groups amongst a plurality of groups, said computer program product comprising a computer usable medium having computer readable program code thereon, said computer readable program code comprising:

computer readable program code means for generating public keys;

computer readable program code means for publishing public keys;

computer readable program code means for generating secure keys that are random suffixes;

computer readable program code means for combining said secure keys with said public keys by concatenating said random suffixes with ones of said plurality of public keys; and

computer readable program code means for selectively distributing a key corresponding to each secure key to members of selected groups.

25. (Currently Amended) A computer program product as in claim 24, wherein the combining means combines said secure keys with said public keys to form secure links in a web page, and further comprising computer readable program code means for changing secure page names including:

computer readable program code means for removing a secure key from said secure page name;

computer readable program code means for attaching a new secure key; and

computer readable program code means for sending e-mail to members of said selected groups, informing said members of said secure name change.

27. (Original) A computer program product as in claim 24, wherein each said secure key is distributed as its corresponding key and the key distribution means comprises:

computer readable program code means for sending each of said secure keys to members of selected ones of said groups, members of at least one said group not being sent at least one distributed key.

28. (Original) A computer program product as in claim 24, further comprising:

computer readable program code means for providing access to secure information responsive to keys provided by group members.

29. (Currently Amended) A computer program product as in claim 28, wherein the computer readable program code means for providing access to secure information further comprises:

computer readable program code means for displaying secure information on a secure web page, each web page containing secure information identified by one of said random suffixes.

30. (Currently Amended) A computer program product as in claim 28, wherein the computer readable program code means for combining the random suffixes with the public keys comprises:

computer readable program code means for creating a plurality of building blocks;

computer readable program code means for attaching a secure key to each of said plurality of building blocks to form secure building blocks; and

computer readable program code means for creating one or more secure web pages, each secure web page including at least one secure building block and having a secure web page name.

31. (Original) A computer program product as in claim 30, wherein the computer readable program code means for selectively distributing the secure keys comprises:

computer readable program code means for sending e-mail to group members and informing said members of said secure web page name.

32. (Original) A computer program product as in claim 31, wherein the computer readable program code means for generating secure keys generates encryption keys and the distributed corresponding keys are decryption keys.

35. (Original) A computer program product as in claim 24, wherein the computer readable program code means for generating random suffixes comprises:

computer readable program code means for generating a plurality of random numbers between 0 and 61; and

computer readable program code means for mapping each of said plurality of random numbers to a corresponding alphanumeric number.

36. (Original) A computer program product as in claim 35, wherein the mapped plurality of random numbers generated is a decryption key, the computer readable program code means for generating random suffixes further comprising:

computer readable program code means for deriving an encryption key from said generated decryption key.

REJECTIONS UNDER 35 U.S.C. 112 FIRST PARAGRAPH

In paragraph 2 of the Office Action, claims 11-13 were rejected as failing to comply with the written description requirement. In response, Applicants amend claim 11 and cancel claim 13 herein to more clearly define the invention, and believe the rejection is overcome.

REJECTIONS UNDER 35 U.S.C. 112 SECOND PARAGRAPH

In paragraphs 4-8 of the Office Action, claims 10-13, 15-18, 20-23, and 30-32 were rejected as indefinite. In response, Applicants cancel claims 13 and 16-18 and amend claims 10-11, 15, 20-21, and 30 herein to more clearly define the invention, and believe the rejections are overcome.

REJECTIONS UNDER 35 U.S.C. 102(e)

In paragraph 10 of the Office Action, claims 1-4, 14-15, 24-25, and 32 were rejected as anticipated by U.S. Pat. No. 6,351,536 to Sasaki. In response, Applicants cancel claims 2 and 4 and amend claims 1, 3, 14-15, and 24-25 herein to more clearly define the invention. Applicants respectfully traverse the rejections as discussed below.

REJECTIONS UNDER 35 U.S.C. 103(a)

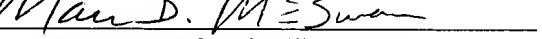
In paragraphs 12, 13, and 14 of the Office Action, claims 5, 7-10, 12, 16-19, 27-29, 31, and 33 were rejected as unpatentable over various combinations of prior art references as detailed above. In response, Applicants cancel claims 5 and 16-18 and amend claims 7-10, 19, 24, and 29 herein to more clearly define the invention. Applicants respectfully traverse the rejections.

Vobach neither teaches nor suggests the use of suffixes as described by the present invention; instead, Vobach uses prefixes and suffixes of pseudo-random integers of predetermined lengths to "pad" ciphertext strings to make the ciphertext difficult to attack by those who intercept it (col. 7, lines 16-23). Win teaches role-based web access, wherein each user's role within an enterprise that controls the resources determines whether access is authorized. (abstract and col. 2 lines 54-56). In contrast, the present invention restricts even the awareness of the availability of sensitive information, so that those parties not intended to have access to the sensitive information are unaware of its availability altogether (page 4 lines 7-9).

All pending claims are now believed to be allowable. Amendments to claims 1 and 24 are believed to encompass the allowable subject matter found in as-filed claims 6, 26, and 34-36. The Examiner is invited to call Applicants' undersigned representative if a telephone conference will expedite the prosecution of this application.

Respectfully submitted,

Nimrod Megiddo et al.

By 

Marc D. McSwain (#44,929)
Phone (408) 927-3364